Laboratorio 1. Plan de la búsqueda sistemática

# Título (Mapeo sistemático de literatura)

Revisión de literatura sobre robo y secuestro de información a través de un ataque cibernético

# Fase 1. Planificación del estudio

# Problema de investigación

Los ataques cibernéticos se caracterizan por la acción de robar, exponer, alterar, deshabilitar o destruir datos mediante el acceso no autorizado a redes, sistemas de información o dispositivos digitales.A cada minuto se realiza un ataque cibernético a nivel mundial a empresas de cualquier tamaño, de los cuales un porcentaje de ataques logra pasar las barreras de seguridad; y cuando esto ocurre, repercute en ellas en costos asociados a la recuperación y la restauración de los sistemas, pueden llegar a ser tan significativos que incluso podrían llevar a la quiebra a su víctima, debido al tiempo de inactividad, la pérdida de ingresos y el daño reputacional a largo plazo.

Este estudio se va a centrar en identificar las empresas que han sido atacadas y que les han robado y/o secuestrado su información corporativa con el fin de analizar por qué fueron víctimas de los ataques.

# Preguntas de investigación

La presente RSL busca responder las siguientes preguntas de investigación:

**P1** ¿Cuáles son las consecuencias para las empresas que no le dan importancia a un ataque cibernético?

**P2** Cómo afectan los ataques cibernéticos a las empresas?

**P3** ¿Cuáles son los países origen de los principales ataques cibernéticos?

**P4** ¿Cuáles son los países que más ataques están sufriendo?

**P5** ¿A qué tipo de riesgos se ven expuestas las empresas después de sufrir un ataque cibernético?

# Selección de fuentes

El objetivo de esta sección es definir las fuentes donde se van a llevar a cabo las búsquedas de los estudios primarios.

En esta sección incluir:

* + 1. Bases de datos seleccionadas para la búsqueda
       1. Scopus
       2. Web of sciencies
    2. Cadenas de búsqueda utilizadas (Si son varias se sugiere presentarlas en una tabla, así como la que se muestra a continuación:

La Tabla 1 muestra una forma de presentar esta parte del plan del estudio.

**Nota**: Se sugiere incluir un párrafo introductorio, así como las bases de datos seleccionadas y las cadenas de búsqueda.

Tabla 1. Cadenas y ecuaciones de búsqueda

|  |  |
| --- | --- |
| **Cadena** | **Cadena de búsqueda** |
| A | ransomware |
| B | “Ransomware protection” |
| C | "Cybersecurity risk" AND "corporate innovation" |
| D | "cyber attack" AND "country" |
| E | " information theft" |

# Criterios de inclusión y exclusión de estudios

En esta sección se deben describir los criterios de inclusión y exclusión que el equipo tendrá en cuenta para la selección de estudios primarios a analizar.

**CI1**. Se incluirán estudios que hablen de empresas que han tenido ataques cibernéticos en los últimos 5 años.

**CI2**. Se incluyen estudios que hablen de los métodos y efectos de la ciberdelincuencia.

**CI3.**Se incluyen estudios que hablen sobre aquellas empresas que les han secuestrado su información.

**CI4.** Se incluyen estudios que su área de estudio esté relacionada con la tecnología

**CE1**.Se excluyen los estudios repetidos en las bases de datos científicas.

**CE2**.Se excluyen estudios que tengan más de 5 años de haber sido publicados.

**CE3**.Se excluyen estudios que no hablen sobre el robo o secuestro de la información.

# Selección de Estudios

Una vez se han identificado las fuentes, es necesario ejecutar las cadenas de búsqueda conformando ecuaciones de búsqueda de acuerdo con las características de cada fuente. Este proceso se debe realizar en cada una de las bases de datos (fuentes) seleccionados para la selección y evaluación de los estudios.

En esta sección se sugiere incluir:

1. En la Tabla 2 se resumen los resultados de las cadenas de búsqueda en las bases de datos seleccionadas así:

Tabla 2. Cantidad de estudios capturados por cadena de búsqeuda

|  |  |  |
| --- | --- | --- |
| **Cadena** | **Scopus** | **Web of sciencies** |
| A | 2289 |  |
| B | 20 |  |
| C | 2 |  |
| D | 677 |  |
| E | 320 |  |

**Tarea 1.** Se espera que en esta sección incluya una una tabla como la Tabla 3 que relacione los estudios filtrados, que es la primera parte del Laboratorio 2. Esta tabla puede ser construida en Excel para su fácil gestión.

Tabla 3. Relación de estudios seleccionados.

|  |  |  |  |
| --- | --- | --- | --- |
| **Nro** | **Titulo Artículo** | **Año** | **Autores** |
| 1 |  |  | En esta columna incluir la referencia del artículo para poder generar la bibliografía. |
| 2 |  |  | (10) |
| 3 |  |  |  |

Referencias

Incluir las referencias de los artículos seleccionados en formato APA (Haciendo uso del gestor bibliográfico Mendeley).

1. Pérez-Díaz NW, Chinchay-Maldonado JO, Mejía-Cabrera HI, Bances-Saavedra DE, Bravo-Ruiz JA. Ransomware Identification Through Sandbox Environment. In: Lecture Notes in Networks and Systems. 2023.

2. Furnell S, Emm D. The ABC of ransomware protection. Computer Fraud and Security. 2017;2017(10).

3. Ali A. Ransomware: A Research and a Personal Case Study of Dealing with this Nasty Malware. Issues in Informing Science and Information Technology. 2017;14.

4. Kamal A, Derbali M, Jan S, Bangash JI, Khan FQ, Jerbi H, et al. A User-friendly Model for Ransomware Analysis Using Sandboxing. Computers, Materials and Continua. 2021;67(3).

5. Infobae. Las 34 empresas que fueron hackeadas en Colombia durante 2022. Infobae. 2023;

6. Trochez Arias IC. Revisión de la clasificación, categorías, métodos y efectos de la ciberdelincuencia en Colombia en la última década. Universidad Santiago de Cali. 2019;

7. Antonio Dussan Clavijo Palabras clave C. Seguridad informática y el malware. Junio) Entramado. 2017;2(1).

8. Quintero Tamayo JF. Usuarios y hackers, un riesgo en la transmisión de datos financieros en Colombia. I+D REVISTA DE INVESTIGACIONES. 2016;2(2).

9. Knapp ED, Langill JT. Hacking Industrial Control Systems. In: Industrial Network Security. 2015.

10. Deterding S, Dixon D, Khaled R, Nacke L. From game design elements to gamefulness: defining gamification. Proceedings of the 15th. 2011;

Aspectos adicionales de interés para la presentación del laboratorio

* 1. Tablas

**Table 1.** Nombre de la tabla ubicado en la parte superior

|  |  |  |
| --- | --- | --- |
| Heading level | Example | Font size and style |
| Title (centered) | **Lecture Notes …** | 14 point, bold |
| 1st-level heading | **1 Introduction** | 12 point, bold |
| 2nd-level heading | **2.1 Printing Area** | 10 point, bold |
| 3rd-level heading | **Headings.** Text follows … | 10 point, bold |
| 4th-level heading | *Remark.* Text follows … | 10 point, italic |

* 1. Figuras

j0157763

**Fig. 1.** Nombre de la figura ubicado en la parte inferior